**UNITED STATES OF AMERICA**

**v.**

**Manning, Bradley E.**
**PFC, U.S. Army,**
**HHC, U.S. Army Garrison,**
**Joint Base Myer-Henderson Hall**
**Fort Myer, Virginia 22211**

**STIPULATION OF EXPECTED TESTIMONY**

**Mr. Albert Janek**

25 **June 2013**

(U) It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Albert Janek were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. (U) I currently work for the Department of State (DoS), Under Secretary of Management, Office for Policy, Right-Sizing, and Innovation, as the Director of Continuity at the United States Embassy in Kabul, Afghanistan. In this capacity, I manage the containment and movement of information at our office in Kabul. I have worked at the DoS for eleven years in various Information Technology (IT) positions. Before joining DoS, I worked in IT for five years for businesses and a university. I possess numerous certifications, including CISSP, CAP, MCSE, Security Plus, A Plus, and Net Plus. I was also a Microsoft Certified Trainer.

2. (U) From 2009 to 2010, I was a Special Projects Manager within the Messaging Systems Products, Messaging Systems Office in the Bureau of Information Research Management, at the DoS. In this capacity, I was responsible for the management of certain DoS Messaging Systems, including Net Centric Diplomacy (NCD) server logs. The NCD server logs track the Internet Protocol (IP) address of a user requesting our resources, as well as the time and date that request was made, whether the user retrieved the resource or not, and the metadata associated with that connection. Metadata is data about data. Structural metadata provides information about the design of data structures. It is essential data about how the data itself is contained. Descriptive metadata is data that provides information about the application of data, or the data content. Accordingly, these server logs describe the connection between two systems on the SIPRNET.

3. (U) A log is created any time a Hypertext Transfer Protocol (HTTP) talks via the Transmission Control Protocol (TCP) and successfully receives information. HTTP is the foundation of data communication for the World Wide Web. It consists of packets of data, which, when connected wirelessly or via Ethernet cable, creates a network for communication. TCP provides reliable, ordered, error-checked delivery of a stream of data between programs running on computers connected to the Internet. Simply put, if TCP is a highway, HTTP constitutes the lanes on the highway. The server logs track the data entering and exiting a server which exists on a classified network platform between the Department of Defense's SIPRNET and the State Department's CLASSNET. Specifically, the NCD Server is located in what is commonly known as the "DMZ" between SIPRNET and the DoS CLASSNET. DoS CLASSNET is the Department's own version of SIPRNET, a classified network that is accredited to hold SECRET information and data. I am aware that the State Department has a "captioning" system for cables. Captions limit the distribution of the cables. A cable could be

PROSECUTION [illegible] 162a for identification
PAGE OFFERED: [illegible] ADMITTED:
PAGE ___ OF ___ PAGES
D2

captioned "STADIS" for distribution to only State Department personnel. It could be captioned "NODIS" for distribution only to the intended recipient. During the time I worked there, a cable could also be captioned "SIPDIS" for distribution on the SIPRNET.

4. (U) I know that these logs are accurate because only three individuals, including myself, had access to them. To alter the data, an individual would have to hack into the server operating system and manipulate the logs. The logs are reviewed about once a quarter, typically to see the number of organizations that are using our products. A log is only created upon a successful request sent to the server. If there is an error, such as "Page Not Available," the log is not created.

5. (U) I first became involved in this case when Special Agent Ellis and Special Agent Bowen of the U.S. Army Criminal Investigation Command (CID) requested that I assist them in the collection of evidence from the server logs of our Net Centric Diplomacy Database (NCD). On 15 June 2010, I assisted them in getting access to the information by escorting the agents to the necessary log-in terminal in the DoS Server Room and logging them into the system using my special permissions. I oversaw the agents as they copied the DoS server logs from January 2009 to June 2009, and from 30 April 2010 to 15 June 2010. Agent Ellis used a forensic tool to pull and compress all of the logs into .zip files. The CID agents saved the logs as "logs.zip" and "newlogs.zip" on a forensically wiped thumb drive. The thumb drive was marked SECRET. I signed the thumb drive over to SA Ellis on a U.S. Department of State Bureau of Diplomatic Security Evidence Receipt/Chain of Custody (Cyber Security Incident Program) form. On that form, I recorded the thumb drive of the files as "files, ZIP, containing logs, filename logs.zip and newlogs.zip, in the root of "D:\", hashed before acquisition and hashed copies, 1232, 15 Jun 10, KNE." The data in these files displays as text. **Prosecution Exhibit (PE) 91 for Identification** is a copy of these logs.

6. (U) If you look at what has been marked as **PE91 for ID**, you can tell the source IP address, the date/time group that the server responded to that source IP's request of the system, what the IP address was requesting, information from the CPU of the source IP address, the protocol, and the search engine and browser used by the source IP address.

7. (U) Below is an explanation of the HTTP logs by column and using a specific line pulled from access_log.2010-05-04.

8. [redacted]

[redacted]

(b) (1) (B)

a. (U) The entry "22.225.41.22" is the source IP address. This address indicates the IP address of the computer where a user is requesting the information.

b. (U) The entry "[04/May/2010:22:04:34 +0000]" is the time and date group, which is given in Zulu Time. The time and date group records when the computer processes the request from the sending IP address.

c. (b) (1) (B)

d. (b) (1) (B)

e. (U) HTTP/1.1 is the protocol, which is discussed above.

f. (U) The entry "200" is a code that states that the user's request to "GET" and access the document was successful.

g. (U) The entry "98796" is a code about the system that the user is connecting from.

h. (b) (1) (B)

i. (U) The entry "%20" means that a space exists in the log.

j. (U) The entry "Mozilla/5.0" tells me that the user of the 22.225.41.22 IP address was using version 5 of the Mozilla browser.

k. (U) The entry "(Windows; U; Windows NT 5.1; en-US; rv:1.9.1.6)" means that a Windows NT workstation was being used by the user of the 22.225.41.22 computer.

l. (U) The entry "Gecko/20091201 Firefox/3.5.6" tells me that the 22.225.41.22 system was using the Firefox browser.

m. (b) (1) (B)

9. (U) I worked on the NCD database for approximately a year. To my knowledge, the NCD database operated in its designed manner for the entire period. In the 2009-2010 timeframe, to my knowledge, there was never any directive for DoS employees to refrain from using the NCD database.

| | | |
|---|---|---|
| //ORIGINAL SIGNED// | //ORIGINAL SIGNED// | //ORIGINAL SIGNED// |
| ANGEL M. OVERGAARD | THOMAS F. HURLEY | BRADLEY E. MANNING |
| CPT, JA | MAJ, JA | PFC, USA |
| Assistant Trial Counsel | Military Defense Counsel | Accused |